

Broadbottom C of E Primary School

E-Safety Policy

School Aims

"Love Learning, Love Life"

We will....

- Love our God, our world, each other and ourselves
- Cherish our pupils, acting as their champions.
- Provide safe yet challenging opportunities to learn, blossom and grow.
- Surround ourselves with fun, laughter, positivity and happiness, creating a place where memories are made.
- Trust each other to act with integrity and to forgive when we make mistakes.
- Love learning and love life

We aim to....

- Be creative in our thinking, outlook and approach
- Communicate effectively
- Give the time needed for stronger growth
- Find each individual's "spark", develop them as thinkers and provide them with the gift of a love of learning and a belief in themselves
- Loves learning and loves life

Rationale

We are excited about the use of new technology.

- The internet provides instant access to a wealth of up-to-the-minute information and resources from across the world, which would not be ordinarily, be available.
- Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.
- Virtual Learning Environments (VLE's) provide children and/or young adults with a platform for personalised and independent learning.

There are many social and educational benefits to be derived including:

- Equipping children with the skills for the future
- Access to a wealth of up-to-date information and resources from across the world through the internet
- Improving children's and/or young adult's reading and research skills
- E-mail, instant messaging and social networking helps to foster and develop good social and communication skills

However there are dangers associated with the Internet and emerging new technologies including:

- Children accessing content of an unsavoury, distressing or offensive nature on the internet
- Children receiving unwanted or inappropriate messages from unknown senders via email or via files sent by Bluetooth. Being exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging.
- Chat rooms provide cover for unscrupulous individuals to groom children.

The benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy, written in accordance with BECTA guidelines, focuses on each individual technology available within the school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Procedures

What users must and must not do when using a PC / laptop connected to the school network.

- Users must access the school network using their own logons and passwords. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software should not be installed, nor programmes downloaded from the Internet, without prior permission from the person responsible for managing the network.
- Only school software to be used on all school hardware including teacher laptops, which may be used at home
- Removable media (e.g. pen drives / memory sticks, CD-ROMs and floppy disks) must not hold downloadable files from the internet
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.
- Our wireless network is encrypted
- Passwords for all office machines are changed half termly

What users must and must not do for safe internet and E-mail use

- All users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.
- Parental or carer consent is requested in pupil planners in order for children to be allowed to use the Internet or email.
- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- The Internet and email must only be used for professional or educational purposes.
- Children must be supervised at all times when using the Internet and email.
- Procedures for Safe Internet use including sanctions applicable if rules are broken, will be clearly displayed beside every computer with access to the Internet.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the person responsible for E-Safety - Mrs. Marrow and a note of the offending website address (URL) taken in red book so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly. Software currently used is Kaspersky
- Internet and email use will be monitored regularly in accordance with the Data Protection Act.
- Users must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from a school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness. Our Anti-virus is Kaspersky.
- All email attachments are scanned before they can be opened.
- Users must seek permission before downloading any files from the Internet.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

Procedures for Use of Instant Messaging (IM), Chat and Weblogs

- The use of Instant Messaging (e.g. MSN messenger) is not permitted.
- Use of Social Networking websites, such as Bebo, MySpace, Facebook, Habbo, and Piczo is not permitted.
- Children/Young adults and staff must not access public or unregulated chat rooms.

Procedures for Use of Cameras, Video Equipment and Webcams

Procedures for safe use of photographic and video equipment.

- **Permission must be obtained in the Pupil Planner from a child's parent or carer before photographs or video footage can be taken.**
- Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be 'password-protected' and accessible only to authorised members of staff.
- Any photographs or video footage stored must be deleted immediately once no longer needed.
- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a 'password-protected' folder onto a school computer immediately upon their return.
- Mobile phones must not be carried by pupils on school premises and must be handed to an adult.
Adults phones must be switched off during school timetabled time.

- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.
- Children / Young adults and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the school's website

- The school has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published. This is Mrs. Bland - Headteacher
- The school website is subject to frequent checks manually to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website.

Names are not used to identify individuals* portrayed in images uploaded onto the school website.

When photographs are used on the website are saved, names of individuals portrayed therein should not be used as file names.

Procedures for using mobile phones and Personal Digital Assistants (PDAs)

- Mobile phones must not be carried by pupils in school, they must be handed to a member of staff
- Mobile phones carried by staff must be turned off during timetables time
- The taking of still pictures or video footage is not permitted without parental permission
- Individuals who are found to use a mobile / camera phone for inappropriate or malicious purposes. I.e. for 'happy-slapping,' the sending of abusive or unsavoury images / text messages or files via Bluetooth, the making of hoax, crank or abusive phone calls, etc. should be reported to the Headteacher. Depending on the nature of the material, she will deal with it appropriately.

• Procedures for Wireless games consoles

Wireless Games consoles are not permitted in school time. Not only might their presence lead to instances of theft, but as children can also connect to the internet and play against other people on-line, they present the same dangers as public chat rooms.

Procedures for using portable media players (e.g. iPods)

The use of iPods is not permitted in school.

Sanctions to be imposed if procedures are not followed

If rules are broken and procedures are not adhered to the following sanctions may be put into place.

- Letters may be sent home to parents or carers (if applicable).
- Users may be suspended from using the school's computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.






Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and that this policy will not remain static. It may be that staff / young adults / children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

Appendices

- i. **Acceptable Use Agreement (AUP) for Staff**
- ii. **Acceptable Use Agreement (AUP) for Pupils / Young adults**
- iii. **Acceptable Use Agreement (AUP) for Guest Users**
- iv. **Risk Assessment Proforma for Emerging Technologies**
- v. **Prevent Statement**

At Broadbottom Primary School we aim to:

- Be aware of and recognise pupils and families in our school community that are at risk of radicalisation.
- To undertake and disseminate any necessary and relevant training to all school staff.
- Report any signs of radicalised behaviour to the relevant bodies either internally to the Senior Management Team or to the relevant external bodies (DfE Guidelines: Keeping Children Safe In Education, September 2015).
- We aim to promote our Christian and British Values including:
 -  Forgiveness
 -  The Rule of Law
 -  Individual Liberty
 -  Mutual Respect
 -  Tolerance for those of different faiths and beliefs